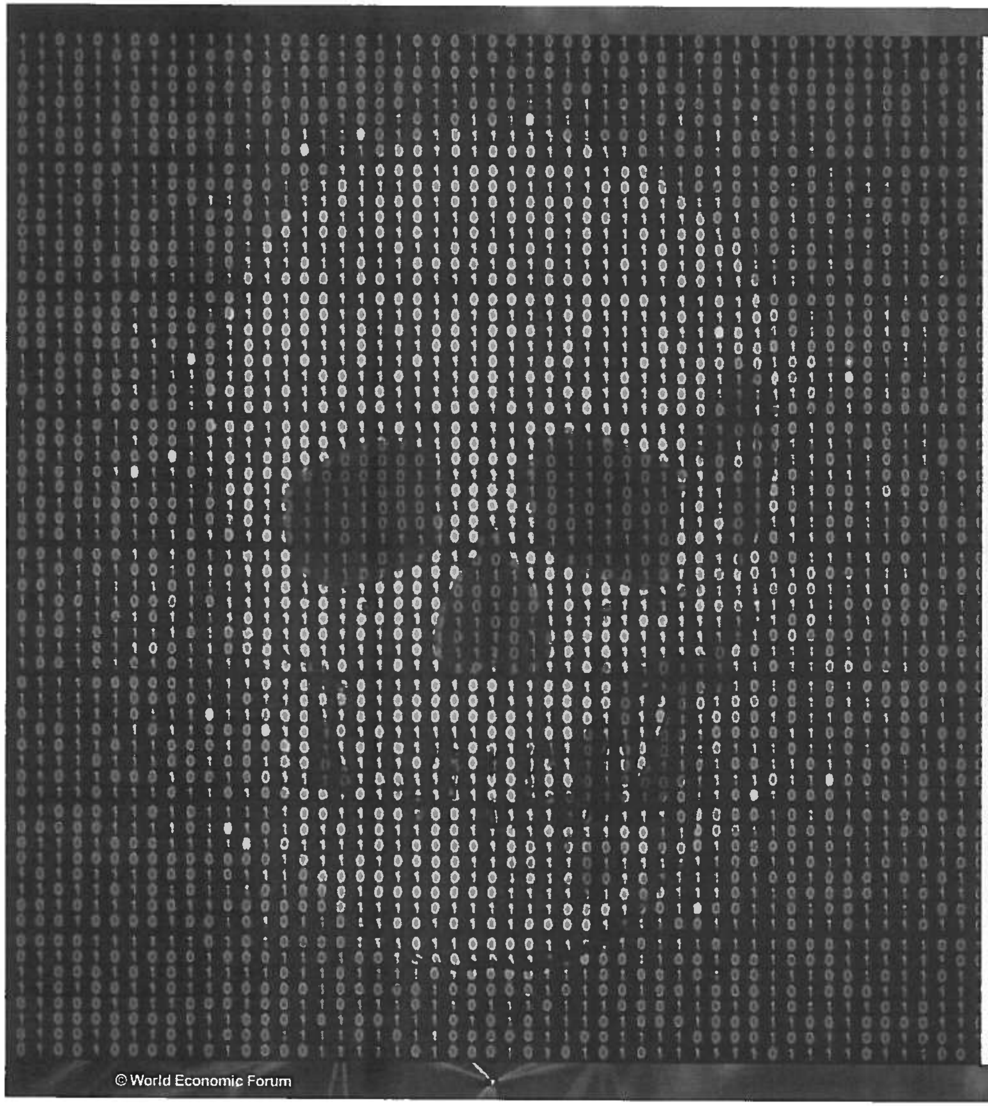
Data as the Hostage
Increasing Cyber-Resilience

Francesca Bosco
Project Lead, Cyber-Resilience

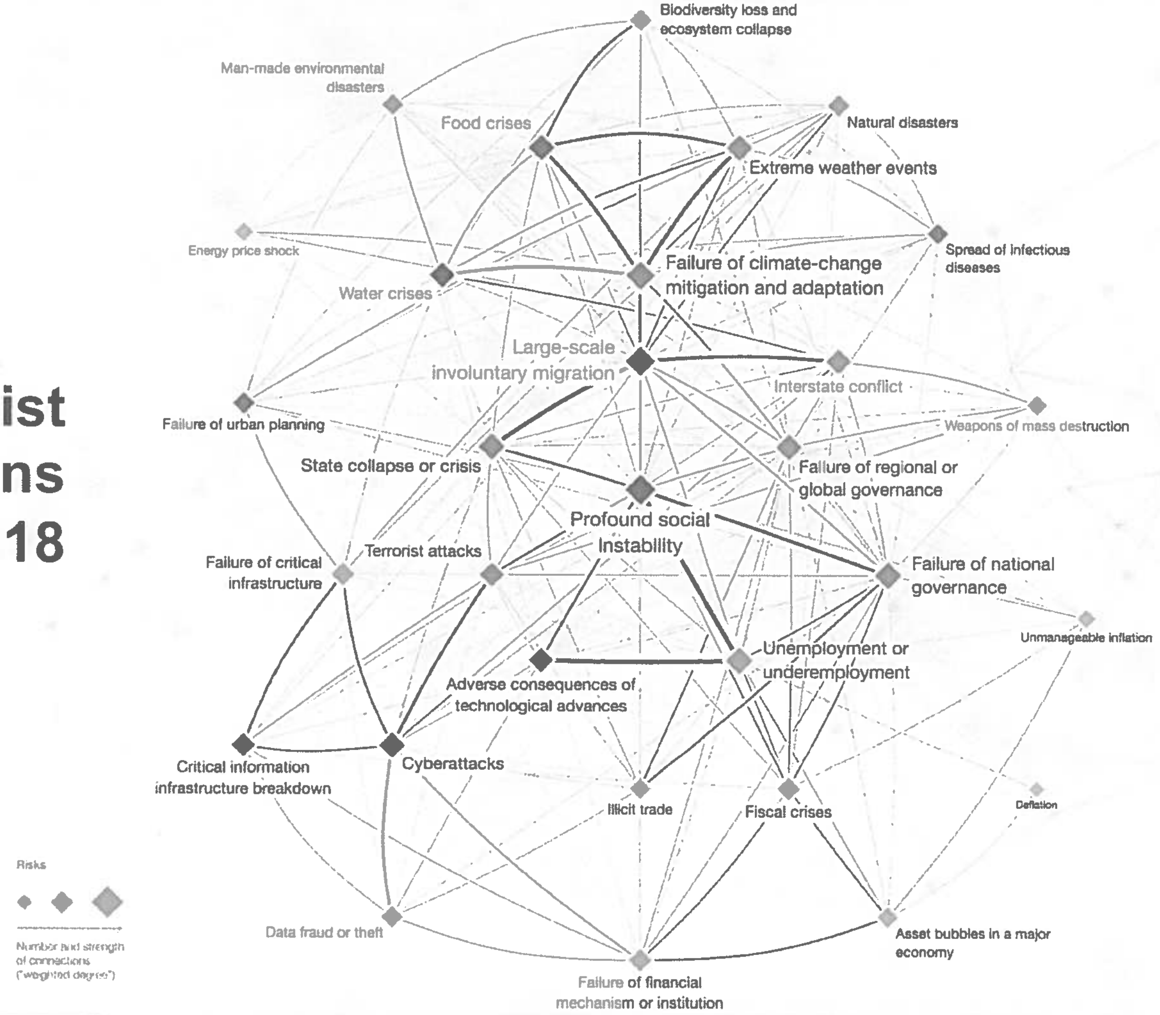
WORLD ECONOMIC FORUM | Centre for Cybersecurity



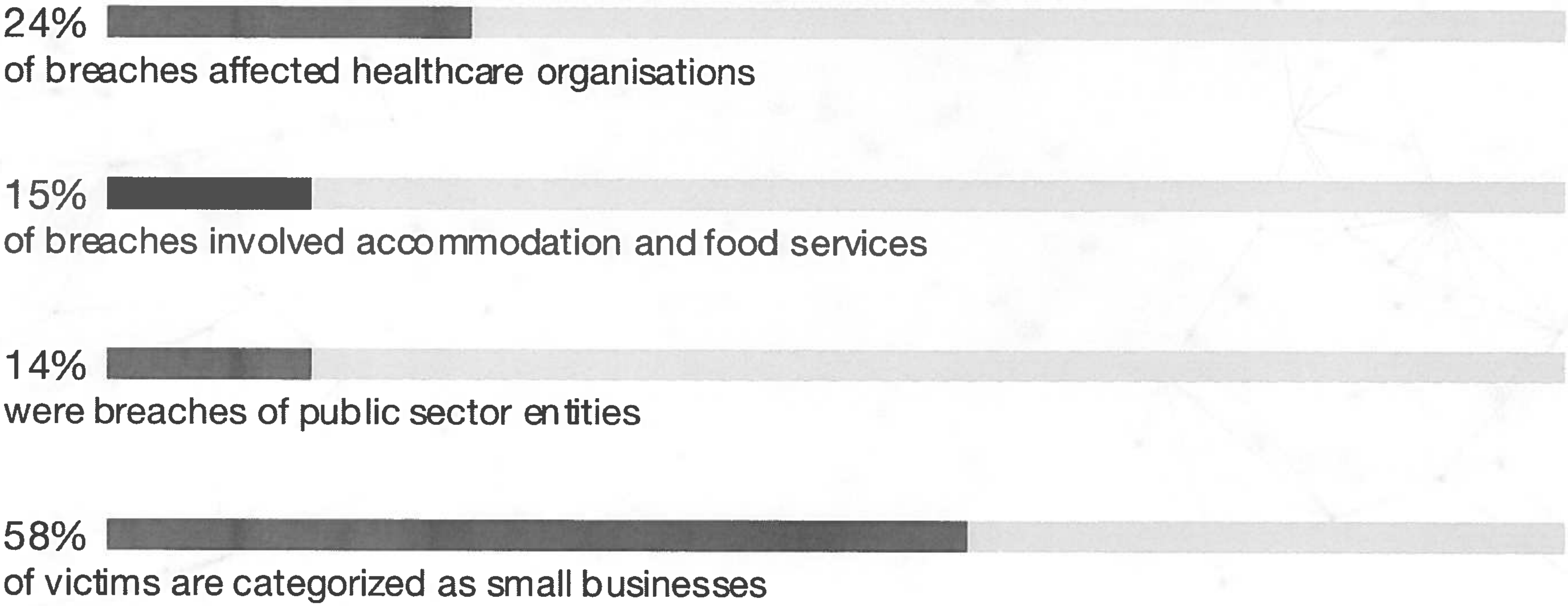
© World Economic Forum

- Changing nature of ransomware
- From a company/single user problem to global consequences
- Re-infection
- Interconnectivity of risks

The Global List Interconnections Map 2018


Biodiversity loss and ecosystem collapse
Man-made environmental disasters
Food crises
Natural disasters
Extreme weather events
Energy price shock
Spread of infectious diseases
Failure of climate-change mitigation and adaptation
Water crises
Large-scale involuntary migration
Interstate conflict
Failure of urban planning
Weapons of mass destruction
State collapse or crisis
Failure of regional or global governance
Profound social instability
Failure of critical infrastructure
Terrorist attacks
Failure of national governance
Unmanageable inflation
Unemployment or underemployment
Adverse consequences of technological advances
Critical information infrastructure breakdown
Cyberattacks
Illicit trade
Fiscal crises
Deflation
Risks
Number and strength of connections ("weighted degree")
Data fraud or theft
Asset bubbles in a major economy
Failure of financial mechanism or institution

Who are the victims?



24%

of breaches affected healthcare organisations

15%

of breaches involved accommodation and food services

14%

were breaches of public sector entities

58%

of victims are categorized as small businesses

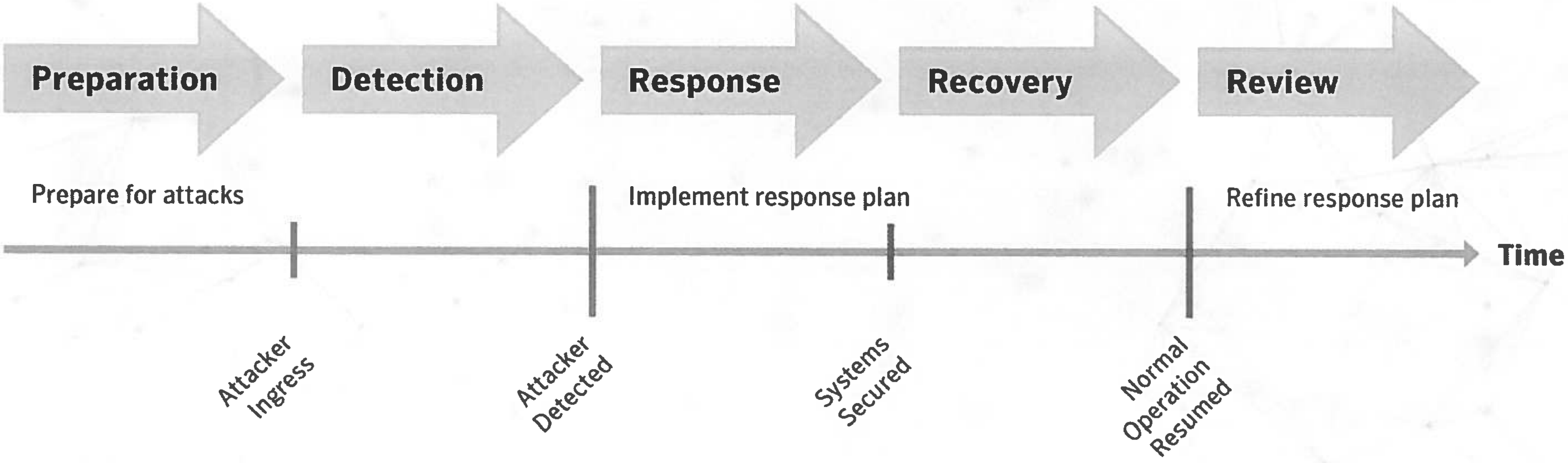
Source 2018: Verizon, Data Breaches Report

Create a Stronger Cyber-Resilience-First and Foremost

Achieve True Visibility Across Your Entire Environment-Map the Assets

1. Maintaining an inventory of authorized and unauthorized devices
2. Maintaining an inventory of authorized and unauthorized software
3. Developing and managing secure configurations for all devices
4. Conducting continuous (automated) vulnerability assessment and remediation
5. Actively managing and controlling the use of administrative privileges

Create a Stronger Cyber-Resilience



Preparation

Detection

Response

Recovery

Review

Prepare for attacks

Implement response plan

Refine response plan

Time

Attacker Ingress

Attacker Detected

Systems Secured

Normal Operation Resumed

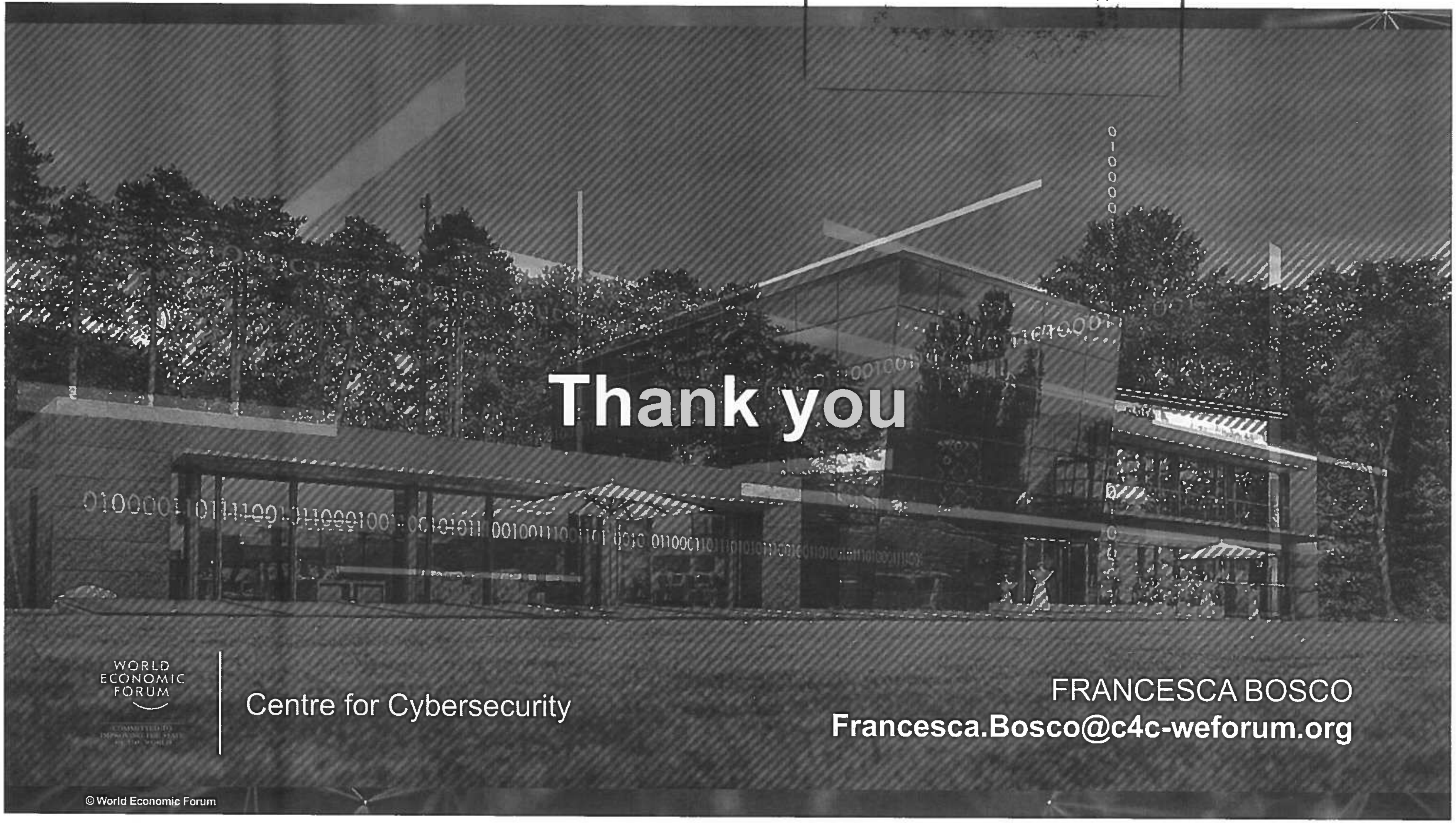
Source 2014:The Cyber Resilience Blueprint: A New Perspective on Security

As C-suite executives and boards prepare their plans for a cyber-resilient business, they need help from the CISO to:

- Understand how the business will have a greater "surface area" of exposure in the future and the impact this has on cyber resilience requirements
- Know what must be done to ensure the future cyber resilience of the business across all dimensions (not just the IT capabilities)
- Be clear on where cyber resilience must reside within the organization
- Understand who in the organization has both overall and individual component responsibility for cyber resilience and who is accountable for it
- Know how to measure cyber resilience exposure and risk with relevant measures and monitor these measures at the highest levels of the organization

Elevate Cyber-Resilience to be a Board-Level Issue

Source 2018: Accenture, State of Cyber Resilience



Thank you

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Centre for Cybersecurity

FRANCESCA BOSCO
Francesca.Bosco@c4c-weforum.org